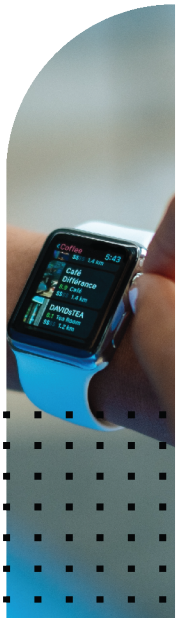
# Release Notes

## FortiSwitchOS 7.0.1



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/support-and-training/training.html

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

June 16, 2021
FortiSwitchOS 7.0.1 Release Notes
11-701-711467-20210616

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| June 16, 2021 | Initial release for FortiSwitchOS 7.0.1 |

# Introduction

This document provides the following information for FortiSwitchOS 7.0.1 build 0038.



See the Fortinet Document Library for FortiSwitchOS documentation.

## Supported models

FortiSwitchOS 7.0.1 supports the following models:

| | |
|---|---|
| **FortiSwitch 1xx** | FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE |
| **FortiSwitch 2xx** | FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE |
| **FortiSwitch 4xx** | FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE |
| **FortiSwitch 5xx** | FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE |
| **FortiSwitch 1xxx** | FS-1024D, FS-1048D, FS-1048E |
| **FortiSwitch 3xxx** | FS-3032D, FS-3032E |
| **FortiSwitch Rugged** | FSR-112D-POE, FSR-124D |

# What's new in FortiSwitchOS 7.0.1

Release 7.0.1 provides the following new features:

- You can now configure VLAN stacking (QnQ) and VLAN mapping in the GUI.
- The Log Entries page (*Log* > *Entries*) has been redesigned to make it easier to read the log messages.
- You can now enable explicit congestion notification (ECN) marking when you create or edit a QoS egress policy in the GUI.
- You can now use the `set fec-state detect-by-module` command to allow split ports of the FS-1048E and FS-3032E models to automatically detect whether forward error correction (FEC) is supported by the module.
- Policy-based routing (PBR) allows users to define the next hop for packets based on the packet's source or destination IP addresses. You can specify the virtual routing and forwarding (VRF) instance that the next hop belongs to or the default VRF instance is used. You can assign the next hop to a next-hop group to use equal-cost multi-path (ECMP) routing.
- The new *Route Diagnostic* page (*Router* > *Diagnostic*) displays a summary of existing routes for a specific IP address or host name and lists the network hops to the specified IP address or host name.
- The new *ARP Table* page (*Router* > *ARP Table*) lists the IP address, number of minutes that the ARP entry has been in the ARP table, MAC address, and interface for each ARP table entry.
- When you add a RADIUS server in the GUI, you can now test if the user credentials for the RADIUS server are valid.
- Equal Cost Multi-Path (ECMP) is now supported by the FS-5xxD models with IPv6.
- You can now specify which switch goes dormant when the split-brain state occurs by setting the priority of each switch. The priority can be 0-100 and is 50 by default. The switch peer with the lowest priority value goes dormant when the split-brain state occurs. If both switch peers have the same priority, the switch with the lowest numerical MAC address goes dormant when the split-brain state occurs.
- You can now force the switch going dormant when the split-brain state occurs to shut down all ports before going dormant. The state of the ICL trunk ports is not changed. By default, this option is disabled.
- Layer-3 IPv4 dynamic routing with MCLAG peer groups is now supported.
- You can now display the VRF IPv6 entries of the routing table.

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

# Special notices

## Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

## Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

**To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:**

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

## Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

# Upgrade information

FortiSwitchOS 7.0.1 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See https://docs.fortinet.com/document/fortiswitch/7.0.0/managed-switch-release-notes.

# Product integration and support

## FortiSwitchOS 7.0.1 support

The following table lists FortiSwitchOS 7.0.1 product integration and support information.

| | |
|---|---|
| **Web browser** | • Mozilla Firefox version 52<br>• Google Chrome version 56<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiOS (FortiLink Support)** | FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later. |

# Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 566433 | Setting the value for `ca-cert` causes LDAP authentication to fail sometimes. |
| 589912 | The version of OpenSSL needs to be upgraded to 1.1.1k. |
| 598871 | Some 4xxE switches report “failed BASE ID Check Sequence” and “failed reading register” errors. |
| 686325 | When many LLDP neighbors are connected to the FortiSwitch units, the daemon receiving the LLDP neighbor messages is overwhelmed and stops synchronizing the configuration. |
| 701196 | The root port for the spanning tree inter-chassis link (ICL) flaps in an MCLAG topology. |
| 704377 | After adding and then removing `ip6-allowaccess ping` from a VRF-enabled switch virtual interface (SVI), ping is still allowed through. |
| 706717 | The first time that the managed FS-108E-FPOE model attempts RADIUS authentication to the Cisco Identity Services Engine (ISE) always fails. |
| 709837 | The number of power supply units on the FS-448D model is not displayed correctly with the `diagnose sys psu status` command. |
| 710229 | When FortiSwitch 802.1x port-based authentication is configured on a switch port with `learning-limit` set to 1, traffic is not received on the FortiGate device. |
| 711074 | After a split-brain state is detected, some of the managed FortiSwitch units in the MCLAG topology are disconnected. |
| 711950 | After upgrading from 6.0.9 to 6.4.5, the FortiGate configuration is not being synchronized with the managed FortiSwitch units. |
| 712323 | After VRRP is enabled, the switch does not respond to ARP requests from the directly connected interface. |
| 715261 | Configuring allow-mac-move for 802.1x authentication does not work when using dynamic VLAN. |
| 719044 | After enabling a MACsec profile for a port, client traffic stopped flowing from that port. |
| 719628 | In an “MCLAG with access rings” topology, the managed switch crashes with an “Unable to handle kernel NULL pointer dereference at virtual address 0000000c” error. |

# Common vulnerabilities and exposures

FortiSwitchOS 7.0.1 is no longer vulnerable to the following CVEs:

- CVE-2021-3449

Visit https://fortiguard.com/psirt for more information.

# Known issues

The following known issues have been identified with FortiSwitchOS 7.0.1. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

| Bug ID | Description |
|---|---|
| 382518, 417024, 417073, 417099, 438441 | DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs). |
| 414972 | IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality. |
| 480605 | When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.<br><br>**Workarounds:**<br>—Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN.<br>—Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping. |
| 510943 | The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.<br><br>**Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables. |
| 542031 | For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs. |
| 548783 | Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources. |
| 572052 | Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.<br><br>**Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x. |
| 585550 | When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded. |
| 606044 | The value for cable length is wrong when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and |

| Bug ID | Description |
|---|---|
| | FS-148E-POE models. |
| 609375 | The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB. |
| 610149 | The results are inaccurate for open and short cables when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models. |
| 617755 | The internal interface cannot obtain IPv6 addresses with dhcpv6-snooping enabled on the native VLAN. |
| 673433 | Some 7-meter DAC cables cause traffic loss for the FS- 448E model. |
| 701560 | The DHCPv6 client cannot get the IP address when VLAN assignment is applied on the FSR-112D-POE model. |

www.fortinet.com